	Department of the Army PRIVACY IMPACT ASSESSMENT (PIA)	ACI^2

RESPONSE FORM

1. DA organizational name (APMS Sub Organization name): **CIDC – Criminal Investigation Command**
2. Name of Information Technology (IT) System (APMS System name): **ACI2 – Automated Criminal Investigation/Criminal Intelligence**
3. Budget System Identification Number (SNAP-IT Initiative Number): **1177**
4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR): **1616**
5. IT Investment (OMB Circular A11) Unique Identifier (if applicable):
6. Privacy Act System of Records Notice Identifier (if applicable): **AO195-2b USACIDC**
7. OMB Information Collection Requirement Number (if applicable) and expiration date:
8. Type of Authority to collect information (statutory or otherwise): **The authority is listed in the federal register notice: 10 USC 3013, AR 195-2, 42 USC 10606 et seq., DoD Directive 1030.1Victum and Witness assistance, and E.O. 9397 (SSN)**
9. Provide a brief summary or overview of the IT system (refer to Encl 2 for description): **The Army Criminal Investigation / Criminal Intelligence system is a system, which allows agents to enter investigative case information and create Reports Of Investigation. Users have the ability to enter information, track case related activity, perform complex searches (subjects, victims, offenses, dispositions) and are able to produce various reports.**
10. Describe what information in identifiable form will be collected and the nature and source of the information: **Information in identifiable form: Name, Social Security Number, rank, date and place of birth; reports of investigation and criminal intelligence reports containing statements of witnesses, suspects, subject and agents; laboratory reports, polygraph reports, documentary evidence, summary and administrative data pertaining to preparation and distribution of the report; basis for allegations; Serious or Sensitive Incident Reports, modus operandi and other investigative information from Federal, State, and local investigative and intelligence agencies and departments. Indices contain codes for the type of crime, location of investigation, year and date of offense, names and personal identifiers of persons who have been subjects of electronic surveillance, suspects, subjects and victims of crimes, report number which allows access to records noted above; and disposition and suspense of offenders listed in criminal investigative**

case files, witness identification data.

11. Describe how the information will be collected:

Investigators gather data from individuals through investigative interviews and through research involving access to a wide variety of other services of information such as automated data systems, records, and third parties.

12. Describe the requirement and why the information in identifiable form is to be collected:

Business and mission critical; USACIDC mission requires gathering information to investigate felony crime related activities to the Army.

CIDC has a responsibility to document/ investigate crimes affecting the Army. The information is collected to properly account for criminal activities and investigation.

13. Describe how the information in identifiable form will be used:

Information is analyzed to determine investigative findings, to refer subjects for adjudication, and to meet regulatory requirements for information reporting to internal and external customers (e.g., name checks, aggregate statistics).

14. Describe whether the system derives or creates new data about individuals through aggregation:

None.

15. Describe with whom the information in identifiable form will be shared, both within DA and outside DA:

Within the Army and DoD: Action Commanders, Staff Judge Advocates, Intelligence agencies, Morale and Welfare, AAFES, and Army Agencies authorized to obtain information for employment and other security concerns. Limited information can be shared in support of the victim/witnesses assistance program.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

Information concerning criminal or possible criminal activity is disclosed to Federal, State, local and/or foreign law enforcement agencies in accomplishing and enforcing criminal laws; analyzing modus operandi, detecting organized criminal activity, or criminal justice employment. Information may also be disclosed to foreign countries under the provisions of the Status of Forces Agreements, or Treaties.

To the Department of Veterans Affairs to verify veterans claims. Criminal investigative files may be used to adjudicate veteran claims for disability benefits, post dramatic stress disorder, and other veteran entitlements.

To Federal, state, and local agencies to comply with the Victim and Witness Assistance Program and the Victims' Rights and Restitution Act of 1990, when the agency is requesting information on behalf of the individual.

To Federal, state, and local law enforcement agencies and private sector entities for the purposes of complying with mandatory background checks, i.e., Brady Handgun Violence Prevention Act (18 U.S.C. 922) and the National Child Protection Act of 1993 (42 U.S.C. 5119 et seq.).

To Federal, state, and local child protection services or family support agencies for the purpose of providing assistance to the individual.

To victims and witnesses of a crime for purposes of providing information, consistent with the requirements of the Victim and Witness Assistance Program, regarding the investigation and disposition of an offense.

To the Immigration and Naturalization Service, Department of Justice, for use in alien admission and naturalization inquiries conducted under Section 105 of the Immigration and Naturalization Act of 1952, as amended.

The DoD 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices also apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form:

None; However, Individuals may refuse to cooperate with investigations as long as their actions do not obstruct justice. Erroneous records may be expunged or corrected by request to Headquarters USACIDC and the Army Board for Correction of Military Records.

17. Describe the process regarding how the individual is to grant consent:

DA Forms 2823 (sworn statement) and DA Form 3881 (rights waiver) provide consent with written warnings and opportunity to object. Other entities may refuse to cooperate with investigations so long as their actions do not obstruct justice.

18. Describe any information that is provided to an individual and the format of such information and means of delivery:

In most cases, individuals must invoke the FOIA/PA to obtain information from the system. Information is sent hardcopy via mail. Some information is provided verbally to individuals through the investigative process, and via victim/witness assistance.

19. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentially of the information in identifiable form:

Only personnel with a need-to-know in order to perform official government duties have access without the consent of the individual. Administrative Security controls include verification that new personnel have a favorable SSBI background investigation and are cleared U.S. citizens, completed initial Information Assurance Security briefing, signed user memorandum of agreement that includes rules for ACI2 system, and completion of user training prior to IASO creating ACI2 account. Individuals must out-process through the IASO and Security, who will then ensure ACI2 account, is disabled. All ACI2 users must complete Annual Information Assurance Security briefing/training. Physical security controls include limiting access to USACIDC offices. All visitors are processed through the Security Office with security guards at the main building entrance and are escorted as required. Outside windows do not open. Technical security controls are employed to minimize unauthorized disclosure, modification, or destruction of data and are in compliance with Army Gold Standard and applicable DoD automated systems security controls requirements. System security controls are reviewed and tested annually at a minimum to ensure compliance.

20. Identify whether the IT system or collection of information will require a System of Records notice. If not published, state when publication of the notice will occur:

N/A, already published.

21. Describe/evaluate any potential privacy risks the collection, use, and sharing of the information in identifiable form:

Due to the stringent safeguards and access requirements the system and data are secure and it is unlikely the data would be compromised or provided to unauthorized individuals or agencies.

22. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals:

Individuals can object to providing information. This complicates and extends the investigative process but relevant data is gathered from other government sources. Individuals are not always afforded the opportunity to object/consent, especially in an ongoing undercover investigation. Notifying individuals at certain times and circumstances could jeopardize the investigative process, judicial actions and put persons at risk of physical harm.

23. Describe/evaluate any risks posed by the adopted security measures:

Controls and mitigations are in place and effective in mitigating all risks to an acceptable level for protecting systems and data up to and including "For Official Use Only" to include Privacy Act data and law enforcement sensitive data as directed. ACI2 system has a current Authority to Operate (ATO) memorandum with an expiration date of 11 May 2009. Due to the stringent safeguards and access requirements the system and data are secure and it is unlikely the data would be compromised or provided to unauthorized individuals or agencies.

24. State classification of information/system and whether the PIA should be published or not. If not, provide rationale:

There is no objection to publishing this PIA.